

Perturbing Eisenstein polynomials over local fields

Kevin Keating
 Department of Mathematics
 University of Florida
 Gainesville, FL 32611
 USA

keating@ufl.edu

January 10, 2017

Abstract

Let K be a local field whose residue field has characteristic p and let L/K be a finite separable totally ramified extension. Let π_L be a uniformizer for L and let $f(X)$ be the minimum polynomial for π_L over K . Suppose $\tilde{\pi}_L$ is another uniformizer for L such that $\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\pi_L^{\ell+2}}$ for some $\ell \geq 1$ and $r \in \mathcal{O}_K$. Let $\tilde{f}(X)$ be the minimum polynomial for $\tilde{\pi}_L$ over K . In this paper we give congruences for the coefficients of $\tilde{f}(X)$ in terms of r and the coefficients of $f(X)$. These congruences improve and extend work of Krasner [7].

1 Introduction

Let K be a field which is complete with respect to a discrete valuation v_K . Let \mathcal{O}_K be the ring of integers of K and let \mathcal{M}_K be the maximal ideal of \mathcal{O}_K . Assume that the residue field $\overline{K} = \mathcal{O}_K/\mathcal{M}_K$ of K is a perfect field of characteristic p . Let K^{sep} be a separable closure of K and let L/K be a finite totally ramified subextension of K^{sep}/K . Let π_L be a uniformizer for L and let

$$f(X) = X^n - c_1X^{n-1} + \cdots + (-1)^{n-1}c_{n-1}X + (-1)^nc_n$$

be the minimum polynomial of π_L over K . Let $\ell \geq 1$, let $r \in \mathcal{O}_K$, and let $\tilde{\pi}_L$ be another uniformizer for L such that $\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{M}_L^{\ell+2}}$. Let

$$\tilde{f}(X) = X^n - \tilde{c}_1X^{n-1} + \cdots + (-1)^{n-1}\tilde{c}_{n-1}X + (-1)^n\tilde{c}_n$$

be the minimum polynomial of $\tilde{\pi}_L$ over K . In this paper we use the techniques developed in [6] to obtain congruences for the coefficients \tilde{c}_i of $\tilde{f}(X)$ in terms of r and the coefficients of $f(X)$.

Let $\phi_{L/K} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ be the Hasse-Herbrand function of L/K , as defined for instance in Chapter IV of [9]. For $1 \leq h \leq n$ set $k_h = \lceil \phi_{L/K}(\ell) + \frac{h}{n} \rceil$. Krasner [7, p.157] showed that for $1 \leq h \leq n$ we have $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^{k_h}}$. In Theorem 4.3 we prove that $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^{k'_h}}$ for certain integers k'_h such that $k'_h \geq k_h$. Let h be the unique integer such that $1 \leq h \leq n$ and n divides $n\phi_{L/K}(\ell) + h$. Krasner [7, p.157] gave a formula for the congruence class modulo $\mathcal{M}_K^{k_h+1}$ of $\tilde{c}_h - c_h$. In Theorem 4.5 we give similar formulas for up to $\nu + 1$ values of h , where $\nu = v_p(n)$.

Heiermann [3] gave formulas which are analogous to the results presented here. Let $S \subset \mathcal{O}_K$ be the set of Teichmüller representatives for \overline{K} . Let π_K be a uniformizer for K and let $\mathcal{F}(X)$ be the unique power series with coefficients in S such that $\pi_K = \pi_L^n \mathcal{F}(\pi_L)$. Suppose $\tilde{\pi}_L$ is another uniformizer for L such that $\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{M}_L^{\ell+2}}$ for some $\ell \geq 1$ and $r \in S$. Let $\tilde{\mathcal{F}}$ be the series with coefficients in S such that $\pi_K = \tilde{\pi}_L^n \tilde{\mathcal{F}}(\tilde{\pi}_L)$. Using Theorem 4.6 of [3] one can compute certain coefficients of $\tilde{\mathcal{F}}$ in terms of r and the coefficients of \mathcal{F} .

In Section 2 and we recall some facts about symmetric polynomials from [6]. The main focus is on expressing monomial symmetric polynomials in terms of elementary symmetric polynomials. In Section 3 we define the indices of inseparability of L/K and some generalizations of the function $\phi_{L/K}$. In Section 4 we prove our main results. In Section 5 we give some examples which illustrate how the theorems from Section 4 are applied.

2 Symmetric polynomials and cycle digraphs

Let $n \geq 1$, let $w \geq 1$, and let $\boldsymbol{\mu}$ be a partition of w . We view $\boldsymbol{\mu}$ as a multiset of positive integers such that the sum $\Sigma(\boldsymbol{\mu})$ of the elements of $\boldsymbol{\mu}$ is equal to w . The cardinality of $\boldsymbol{\mu}$ is denoted by $|\boldsymbol{\mu}|$. For $\boldsymbol{\mu}$ such that $|\boldsymbol{\mu}| \leq n$ we let $m_{\boldsymbol{\mu}}(X_1, \dots, X_n)$ be the monomial symmetric polynomial in n variables associated to $\boldsymbol{\mu}$. For $1 \leq h \leq n$ let $e_h(X_1, \dots, X_n)$ denote the elementary symmetric polynomial of degree h in n variables. By the fundamental theorem of symmetric polynomials there is a unique polynomial $\psi_{\boldsymbol{\mu}} \in \mathbb{Z}[X_1, \dots, X_n]$ such that $m_{\boldsymbol{\mu}} = \psi_{\boldsymbol{\mu}}(e_1, \dots, e_n)$. In this section we use a theorem of Kulikaukas and Remmel [8] to compute certain coefficients of $\psi_{\boldsymbol{\mu}}$.

The formula of Kulikaukas and Remmel can be expressed in terms of tilings of a certain type of digraph. We say that a directed graph Γ is a cycle digraph if it is a disjoint union of finitely many directed cycles of length ≥ 1 . We denote the vertex set of Γ by $V(\Gamma)$, and we define the sign of Γ to be $\text{sgn}(\Gamma) = (-1)^{w-c}$, where $w = |V(\Gamma)|$ and c is the number of cycles that make up Γ .

Let Γ be a cycle digraph with $w \geq 1$ vertices and let $\boldsymbol{\lambda}$ be a partition of w . A $\boldsymbol{\lambda}$ -tiling of Γ is a set S of subgraphs of Γ such that

1. Each $\gamma \in S$ is a directed path of length ≥ 0 .
2. The collection $\{V(\gamma) : \gamma \in S\}$ forms a partition of the set $V(\Gamma)$.
3. The multiset $\{|V(\gamma)| : \gamma \in S\}$ is equal to $\boldsymbol{\lambda}$.

Let μ be another partition of w . A (λ, μ) -tiling of Γ is an ordered pair (S, T) , where S is a λ -tiling of Γ and T is a μ -tiling of Γ . Let Γ' be another cycle digraph with w vertices and let (S', T') be a (λ, μ) -tiling of Γ' . An isomorphism from (Γ, S, T) to (Γ', S', T') is an isomorphism of digraphs $\theta : \Gamma \rightarrow \Gamma'$ which carries S onto S' and T onto T' . Say that the (λ, μ) -tilings (S, T) and (S', T') of Γ are isomorphic if there exists an isomorphism from (Γ, S, T) to (Γ, S', T') . Say that (S, T) is an admissible (λ, μ) -tiling of Γ if (Γ, S, T) has no nontrivial automorphisms. Let $\eta_{\lambda\mu}(\Gamma)$ denote the number of isomorphism classes of admissible (λ, μ) -tilings of Γ .

Let $w \geq 1$ and let λ, μ be partitions of w . Set

$$d_{\lambda\mu} = (-1)^{|\lambda|+|\mu|} \cdot \sum_{\Gamma} \text{sgn}(\Gamma) \eta_{\lambda\mu}(\Gamma), \quad (2.1)$$

where the sum is over all isomorphism classes of cycle digraphs Γ with w vertices. Since $\eta_{\mu\lambda} = \eta_{\lambda\mu}$ we have $d_{\mu\lambda} = d_{\lambda\mu}$. Kulikauskas and Remmel [8, Th. 1(ii)] proved the following:

Theorem 2.1 *Let $n \geq 1$, let $w \geq 1$, and let μ be a partition of w with at most n parts. Let ψ_{μ} be the unique element of $\mathbb{Z}[X_1, \dots, X_n]$ such that $m_{\mu} = \psi_{\mu}(e_1, \dots, e_n)$. Then*

$$\psi_{\mu}(X_1, \dots, X_n) = \sum_{\lambda} d_{\lambda\mu} \cdot X_{\lambda_1} X_{\lambda_2} \dots X_{\lambda_k},$$

where the sum is over all partitions $\lambda = \{\lambda_1, \dots, \lambda_k\}$ of w such that $1 \leq \lambda_i \leq n$ for $1 \leq i \leq k$.

We now recall some formulas from [6] for computing values of $\eta_{\lambda\mu}(\Gamma)$.

Proposition 2.2 *Let a, b, c, d, w be positive integers such that $a \neq c$, $b \neq d$, and let r, s be nonnegative integers. Let Γ be a directed cycle of length w .*

(a) *Suppose $w = ra = sb + d$. Let λ be the partition of w consisting of r copies of a , and let μ be the partition of w consisting of s copies of b and one copy of d . Then $\eta_{\lambda\mu}(\Gamma) = a$.*

(b) *Suppose $w = ra + c = sb + d$. Let λ be the partition of w consisting of r copies of a and one copy of c , and let μ be the partition of w consisting of s copies of b and one copy of d . Then $\eta_{\lambda\mu}(\Gamma) = w$.*

Proof: Statement (a) follows from Proposition 2.5 of [6] if $s = 0$, and from Proposition 2.3 of [6] if $s \geq 1$. Statement (b) follows from Proposition 2.2 of [6]. \square

Using these formulas we can compute $d_{\lambda\mu}$ in some cases.

Proposition 2.3 *Let a, b, c, d, w be positive integers such that $a \neq c$ and $b \neq d$. Let r, s be nonnegative integers such that $w = ra + c = sb + d$ and $a > sb$. Let λ be the*

partition of w consisting of r copies of a and 1 copy of c , and let μ be the partition of w consisting of s copies of b and 1 copy of d . Then

$$d_{\lambda\mu} = \begin{cases} (-1)^{r+s+w+1}w & \text{if } b \nmid c \text{ or } sb < c, \\ (-1)^{r+s+w+1}(w - ab) & \text{if } b \mid c \text{ and } sb \geq c. \end{cases}$$

Proof: Let Γ be a cycle digraph which has an admissible (λ, μ) -tiling. Suppose Γ consists of a single cycle of length w . Then by Proposition 2.2(b) we have $\eta_{\lambda\mu}(\Gamma) = w$. Suppose Γ has more than one cycle. Since Γ has a μ -tiling, Γ has a cycle Γ_1 such that $|V(\Gamma_1)| \leq sb$. Since $a > sb$ and Γ has a λ -tiling, it follows that $|V(\Gamma_1)| = c = mb$ for some m such that $1 \leq m \leq s$. Hence if Γ has more than one cycle we must have $b \mid c$ and $c \leq sb$. Let λ_1 be the partition of c consisting of one copy of c and let μ_1 be the partition of c consisting of m copies of b . Then every λ -tiling of Γ restricts to a λ_1 -tiling of Γ_1 , and every μ -tiling of Γ restricts to a μ_1 -tiling of Γ_1 . It follows from Proposition 2.2(a) that $\eta_{\lambda_1\mu_1}(\Gamma_1) = b$.

Let Γ_2 be another cycle of Γ . Since Γ has a λ -tiling, $|V(\Gamma_2)| \geq a > sb$. Hence every μ -tiling of Γ restricts to a tiling of Γ_2 which includes a path δ with $|V(\delta)| = d$. Since μ has only one part equal to d , it follows that $\Gamma = \Gamma_1 \cup \Gamma_2$. Therefore we have $|V(\Gamma_2)| = ra = (s - m)b + d$. Let λ_2 be the partition of ra consisting of r copies of a and let μ_2 be the partition of $(s - m)b + d = ra$ consisting of $s - m$ copies of b and 1 copy of d . Then every λ -tiling of Γ restricts to a λ_2 -tiling of Γ_2 , and every μ -tiling of Γ restricts to a μ_2 -tiling of Γ_2 . It follows from Proposition 2.2(a) that $\eta_{\lambda_2\mu_2}(\Gamma_2) = a$. Hence

$$\eta_{\lambda\mu}(\Gamma) = \eta_{\lambda_1\mu_1}(\Gamma_1) \cdot \eta_{\lambda_2\mu_2}(\Gamma_2) = ba.$$

Suppose $b \nmid c$ or $c > sb$. Then it follows from the above that the only cycle digraph which has a (λ, μ) -tiling consists of a single cycle of length w . Hence by (2.1) we get

$$d_{\lambda\mu} = (-1)^{(r+1)+(s+1)} \cdot (-1)^{w-1}w.$$

Suppose $b \mid c$ and $sb \geq c$. Then $c = mb$ with $1 \leq m \leq s$. Hence there are two cycle digraphs which have a (λ, μ) -tiling: a single cycle of length w , and the union of two cycles with lengths $c = mb$ and $ra = (s - m)b + d$. Therefore by (2.1) we get

$$d_{\lambda\mu} = (-1)^{(r+1)+(s+1)}((-1)^{w-1}w + (-1)^{w-2}ab).$$

Hence the formula for $d_{\lambda\mu}$ given in the theorem holds in both cases. \square

We recall some results from [6] regarding the p -adic properties of the coefficients $d_{\lambda\mu}$. Let $w \geq 1$ and let λ be a partition of w . For $k \geq 1$ let $k * \lambda$ be the partition of kw which is the multiset sum of k copies of λ , and let $k \cdot \lambda$ be the partition of kw obtained by multiplying the parts of λ by k .

Proposition 2.4 *Let $t \geq j \geq 0$, let $w' \geq 1$, and set $w = w'p^t$. Let λ' be a partition of w' and set $\lambda = p^t \cdot \lambda'$. Let μ be a partition of w such that there does not exist a partition μ' with $\mu = p^{j+1} * \mu'$. Then p^{t-j} divides $d_{\lambda\mu}$.*

Proof: This is proved in Corollary 3.4 of [6]. \square

Proposition 2.5 *Let $w' \geq 1$, $j \geq 1$, and $t \geq 0$. Let λ', μ' be partitions of w' such that the parts of λ' are all divisible by p^t . Set $w = w'p^j$, so that $\lambda = p^j \cdot \lambda'$ and $\mu = p^j * \mu'$ are partitions of w . Then $d_{\lambda\mu} \equiv d_{\lambda'\mu'} \pmod{p^{t+1}}$.*

Proof: This is proved in Proposition 3.5 of [6]. \square

3 Indices of inseparability

Let L/K be a totally ramified extension of degree $n = up^\nu$, with $p \nmid u$. Let π_L be a uniformizer for L whose minimum polynomial over K is

$$f(X) = X^n - c_1X^{n-1} + \cdots + (-1)^{n-1}c_{n-1}X + (-1)^nc_n.$$

For $k \in \mathbb{Z}$ define $\bar{v}_p(k) = \min\{v_p(k), \nu\}$. For $0 \leq j \leq \nu$ set

$$\begin{aligned} i_j^{\pi_L} &= \min\{nv_K(c_h) - h : 1 \leq h \leq n, \bar{v}_p(h) \leq j\} \\ &= \min\{v_L(c_h\pi_L^{n-h}) : 1 \leq h \leq n, \bar{v}_p(h) \leq j\} - n. \end{aligned} \quad (3.1)$$

Then $i_j^{\pi_L}$ is either a nonnegative integer or ∞ ; if $\text{char}(K) = p$ then $i_j^{\pi_L}$ must be finite, since L/K is separable. Let $e_L = v_L(p)$ denote the absolute ramification index of L . We define the j th index of inseparability of L/K to be

$$i_j = \min\{i_{j'}^{\pi_L} + (j' - j)e_L : j \leq j' \leq \nu\}. \quad (3.2)$$

By Proposition 3.12 and Theorem 7.1 of [3], i_j does not depend on the choice of π_L . Furthermore, our definition of i_j agrees with Definition 7.3 in [3]; for the characteristic- p case see also [1, pp. 232–233] and [2, §2]. Write $i_j = A_jn - b_j$ with $1 \leq b_j \leq n$.

Remark 3.1 If $i_j^{\pi_L}$ is finite we can write $i_j^{\pi_L} = a_jn - b_j$ with $a_j \geq 1$ (see Section 4 of [6]). Thus if $i_j = i_{j'}^{\pi_L} + (j' - j)e_L$ then $A_j = a_{j'} + (j' - j)e_K$.

The following facts are easy consequences of the definitions:

1. $0 = i_\nu < i_{\nu-1} \leq \cdots \leq i_1 \leq i_0 < \infty$.
2. If $\text{char}(K) = p$ then $i_j = i_j^{\pi_L}$.
3. Let $m = \bar{v}_p(i_j)$. If $m \leq j$ then $i_j = i_m = i_j^{\pi_L} = i_m^{\pi_L}$. If $m > j$ then $\text{char}(K) = 0$ and $i_j = i_m^{\pi_L} + (m - j)e_L$.

Following [3, (4.4)], for $0 \leq j \leq \nu$ we define functions $\tilde{\phi}_j : [0, \infty) \rightarrow [0, \infty)$ by $\tilde{\phi}_j(x) = i_j + p^jx$. The generalized Hasse-Herbrand functions $\phi_j : [0, \infty) \rightarrow [0, \infty)$ are then defined by

$$\phi_j(x) = \min\{\tilde{\phi}_{j_0}(x) : 0 \leq j_0 \leq j\}. \quad (3.3)$$

Hence we have $\phi_j(x) \leq \phi_{j'}(x)$ for $0 \leq j' \leq j$. Let $\phi_{L/K} : [0, \infty) \rightarrow [0, \infty)$ be the usual Hasse-Herbrand function. Then by Corollary 6.11 of [3] we have $\phi_\nu(x) = n\phi_{L/K}(x)$.

For a partition $\lambda = \{\lambda_1, \dots, \lambda_k\}$ whose parts satisfy $1 \leq \lambda_i \leq n$ define $c_\lambda = c_{\lambda_1}c_{\lambda_2} \cdots c_{\lambda_k}$. The following is proved in Proposition 4.2 of [6].

Proposition 3.2 *Let $w \geq 1$ and let $\lambda = \{\lambda_1, \dots, \lambda_k\}$ be a partition of w whose parts satisfy $1 \leq \lambda_i \leq n$. Choose q to minimize $\bar{v}_p(\lambda_q)$ and set $t = \bar{v}_p(\lambda_q)$. Then $v_L(c_\lambda) \geq i_t^{\pi_L} + w$. If $v_L(c_\lambda) = i_t^{\pi_L} + w$ and $i_t^{\pi_L} < \infty$ then $\lambda_q = b_t$ and $\lambda_i = b_\nu = n$ for all $i \neq q$.*

4 Perturbing π_L

In this section we prove our main theorems. We begin by applying the results of Section 2 to the totally ramified extension L/K . Write $[L : K] = n = up^\nu$ with $p \nmid u$. Let $\pi_L, \tilde{\pi}_L$ be uniformizers for L , with minimum polynomials over K given by

$$\begin{aligned} f(X) &= X^n - c_1 X^{n-1} + \dots + (-1)^{n-1} c_{n-1} X + (-1)^n c_n \\ \tilde{f}(X) &= X^n - \tilde{c}_1 X^{n-1} + \dots + (-1)^{n-1} \tilde{c}_{n-1} X + (-1)^n \tilde{c}_n. \end{aligned}$$

Let $1 \leq h \leq n$ and set $j = \bar{v}_p(h)$. Define a function $\rho_h : \mathbb{N} \rightarrow \mathbb{N}$ by

$$\rho_h(\ell) = \left\lceil \frac{\phi_j(\ell) + h}{n} \right\rceil.$$

Let $\ell \geq 1$. We say $\tilde{f} \sim_\ell f$ if $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^{\rho_h(\ell)}}$ for $1 \leq h \leq n$. Thus \sim_ℓ is an equivalence relation on the set of minimum polynomials over K for uniformizers of L .

Let $\sigma_1, \dots, \sigma_n$ be the K -embeddings of L into K^{sep} . For each partition μ with at most n parts define $M_\mu : L \rightarrow K$ by

$$M_\mu(\alpha) = m_\mu(\sigma_1(\alpha), \dots, \sigma_n(\alpha)).$$

For $1 \leq h \leq n$ define $E_h : L \rightarrow K$ by

$$E_h(\alpha) = e_h(\sigma_1(\alpha), \dots, \sigma_n(\alpha)).$$

Then $c_h = E_h(\pi_L)$ and $\tilde{c}_h = E_h(\tilde{\pi}_L)$.

Proposition 4.1 *Let $\phi(X) = r_1 X + r_2 X^2 + \dots$ be a power series with coefficients in \mathcal{O}_K such that $\tilde{\pi}_L = \phi(\pi_L)$. Then for $1 \leq h \leq n$ we have*

$$E_h(\tilde{\pi}_L) = \sum_{\mu} r_{\mu_1} r_{\mu_2} \dots r_{\mu_h} M_\mu(\pi_L),$$

where the sum ranges over all partitions $\mu = \{\mu_1, \dots, \mu_h\}$ with h parts.

Proof: This is a special case of Proposition 4.4 in [6]. □

Proposition 4.2 *Let $n \geq 1$, let $w \geq 1$, and let μ be a partition of w with at most n parts. Then*

$$M_\mu(\pi_L) = \sum_{\lambda} d_{\lambda\mu} c_\lambda,$$

where the sum is over all partitions $\lambda = \{\lambda_1, \dots, \lambda_k\}$ of w such that $1 \leq \lambda_i \leq n$ for $1 \leq i \leq k$.

Proof: This follows from Theorem 2.1 by setting $X_i = E_i(\pi_L) = c_i$. \square

Let $\ell \geq 1$. Our first main result gives congruences between the coefficients of $f(X)$ and the coefficients of $\tilde{f}(X)$ under the assumption $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{M}_L^{\ell+1}}$.

Theorem 4.3 *Let $\pi_L, \tilde{\pi}_L$ be uniformizers for L and let $f(X), \tilde{f}(X)$ be the minimum polynomials for $\pi_L, \tilde{\pi}_L$ over K . Suppose there are $\ell \geq 1$ and $\sigma \in \text{Aut}_K(L)$ such that $\sigma(\tilde{\pi}_L) \equiv \pi_L \pmod{\mathcal{M}_L^{\ell+1}}$. Then $\tilde{f} \sim_\ell f$.*

Proof: We first show that the theorem holds in the case where $\tilde{\pi}_L = \pi_L + r\pi_L^{\ell+1}$, with $r \in \mathcal{O}_K$. Let $1 \leq h \leq n$ and set $j = \bar{v}_p(h)$. For $0 \leq s \leq h$ let μ_s be the partition of $\ell s + h$ consisting of $h - s$ copies of 1 and s copies of $\ell + 1$. Then by Proposition 4.1 we have

$$\tilde{c}_h = E_h(\tilde{\pi}_L) = \sum_{s=0}^h M_{\mu_s}(\pi_L) r^s = c_h + \sum_{s=1}^h M_{\mu_s}(\pi_L) r^s. \quad (4.1)$$

To prove that $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^{\rho_h(\ell)}}$ it's enough to show that $v_K(M_{\mu_s}(\pi_L)) \geq \rho_h(\ell)$ for $1 \leq s \leq h$. Therefore by Proposition 4.2 it suffices to show $v_L(d_{\lambda\mu_s} c_\lambda) \geq \phi_j(\ell) + h$ for all $1 \leq s \leq h$ and all partitions λ of $\ell s + h$ whose parts are at most n .

Let $1 \leq s \leq h$, set $j = \bar{v}_p(h)$, and set $m = \min\{j, \bar{v}_p(s)\}$. Then $m \leq j$ and $s \geq p^m$. Let $\lambda = \{\lambda_1, \dots, \lambda_k\}$ be a partition of $\ell s + h$ such that $1 \leq \lambda_i \leq n$ for $1 \leq i \leq k$. Choose q to minimize $\bar{v}_p(\lambda_q)$ and set $t = \bar{v}_p(\lambda_q)$. By Proposition 3.2 we have $v_L(c_\lambda) \geq i_t^{\pi_L} + \ell s + h$. Suppose $m < t$. Then $m < \nu$, so we have $p^{m+1} \nmid \gcd(h - s, s)$. Hence by Proposition 2.4 we get $v_p(d_{\lambda\mu_s}) \geq t - m$. Thus

$$\begin{aligned} v_L(d_{\lambda\mu_s} c_\lambda) &= v_L(d_{\lambda\mu_s}) + v_L(c_\lambda) \\ &\geq (t - m)v_L(p) + i_t^{\pi_L} + \ell s + h \\ &\geq i_m + \ell p^m + h. \end{aligned}$$

Suppose $m \geq t$. Then

$$\begin{aligned} v_L(d_{\lambda\mu_s} c_\lambda) &\geq v_L(c_\lambda) \\ &\geq i_t^{\pi_L} + \ell s + h \\ &\geq i_t + \ell p^m + h \\ &\geq i_m + \ell p^m + h. \end{aligned}$$

In both cases we get $v_L(d_{\lambda\mu_s} c_\lambda) \geq \tilde{\phi}_m(\ell) + h \geq \phi_j(\ell) + h$, and hence $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^{\rho_h(\ell)}}$. Since this holds for $1 \leq h \leq n$ we get $\tilde{f} \sim_\ell f$.

We now prove the general case. Since \tilde{f} is the minimum polynomial of $\sigma(\tilde{\pi}_L)$ over K we may assume without loss of generality that $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{M}_L^{\ell+1}}$. By repeated application of the special case above we get a sequence $\pi_L^{(0)} = \pi_L, \pi_L^{(1)}, \pi_L^{(2)}, \dots$ of uniformizers for L with minimum polynomials $f^{(0)} = f, f^{(1)}, f^{(2)}, \dots$ such that for all $i \geq 0$ we have $\pi_L^{(i)} \equiv \tilde{\pi}_L \pmod{\mathcal{M}_L^{\ell+i+1}}$ and $f^{(i+1)} \sim_{\ell+i} f^{(i)}$. It follows that $f^{(i+1)} \sim_\ell f^{(i)}$, and hence that $f^{(i)} \sim_\ell f$ for all $i \geq 0$. Since the sequence $(f^{(i)})$ converges coefficientwise to \tilde{f} it follows that $\tilde{f} \sim_\ell f$. \square

Remark 4.4 It follows from Theorem 4.3 that if $\sigma(\tilde{\pi}_L) \equiv \pi_L \pmod{\mathcal{M}_L^{\ell+1}}$ for some $\sigma \in \text{Aut}_K(L)$ then $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^{\rho_h(\ell)}}$ for $1 \leq h \leq n$. Define functions $\kappa_h : \mathbb{N} \rightarrow \mathbb{N}$ by

$$\kappa_h(\ell) = \left\lceil \frac{\phi_\nu(\ell) + h}{n} \right\rceil.$$

Krasner [7, p.157] showed that $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^{\kappa_h(\ell)}}$. Since $\kappa_h(\ell) \leq \rho_h(\ell)$ Krasner's congruences are in general weaker than the congruences that follow from Theorem 4.3. However, if ℓ is greater than or equal to the largest lower ramification break of L/K then $\phi_j(\ell) = \phi_\nu(\ell)$ for $0 \leq j \leq \nu$. Therefore Theorem 4.3 does not improve on [7] in these cases.

For certain values of h we get a more refined version of the congruences that follow from Theorem 4.3.

Theorem 4.5 *Let L/K be a finite totally ramified extension of degree $n = up^\nu$. For $0 \leq m \leq \nu$ write the m th index of inseparability of L/K in the form $i_m = A_m n - b_m$ with $1 \leq b_m \leq n$. Let $\pi_L, \tilde{\pi}_L$ be uniformizers for L such that there are $\ell \geq 1, r \in \mathcal{O}_K$, and $\sigma \in \text{Aut}_K(L)$ with $\sigma(\tilde{\pi}_L) \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{M}_L^{\ell+2}}$. Let $0 \leq j \leq \nu$ satisfy $\bar{v}_p(\phi_j(\ell)) = j$, and let h be the unique integer such that $1 \leq h \leq n$ and n divides $\phi_j(\ell) + h$. Set $k = (\phi_j(\ell) + h)/n$ and $h_0 = h/p^j$. Then*

$$\tilde{c}_h \equiv c_h + \sum_{m \in S_j} g_m c_n^{k-A_m} c_{b_m} r^{p^m} \pmod{\mathcal{M}_K^{k+1}},$$

where

$$S_j = \{m : 0 \leq m \leq j, \phi_j(\ell) = \tilde{\phi}_m(\ell)\}$$

$$g_m = \begin{cases} (-1)^{k+\ell+A_m}(h_0 p^{j-m} + \ell - up^{\nu-m}) & \text{if } b_m < h \\ (-1)^{k+\ell+A_m}(h_0 p^{j-m} + \ell) & \text{if } h \leq b_m < n \\ (-1)^{k+\ell+A_m}up^{\nu-m} & \text{if } b_m = n. \end{cases}$$

Proof: We first prove that the theorem holds for $\hat{\pi}_L = \pi_L + r\pi_L^{\ell+1}$. Let

$$\hat{f}(X) = X^n - \hat{c}_1 X^{n-1} + \cdots + (-1)^{n-1} \hat{c}_{n-1} X + (-1)^n \hat{c}_n$$

be the minimum polynomial for $\hat{\pi}_L$ over K . Let $1 \leq s \leq h$ and let λ be a partition of $\ell s + h$ whose parts are at most n . Choose q to minimize $\bar{v}_p(\lambda_q)$ and set $t = \bar{v}_p(\lambda_q)$. Recall that μ_s is the partition of $\ell s + h$ consisting of $h-s$ copies of 1 and s copies of $\ell+1$. Since $\bar{v}_p(h) = \bar{v}_p(\phi_j(\ell)) = j$ it follows from the proof of Theorem 4.3 that $v_K(d_{\lambda\mu_s} c_\lambda) \geq k$. Suppose $v_K(d_{\lambda\mu_s} c_\lambda) = k$. Then the inequalities in the proof of Theorem 4.3 must be equalities. Hence there is $0 \leq m \leq j$ such that $s = p^m$, $v_L(c_\lambda) = i_t^{\pi_L} + \ell p^m + h$, and $\phi_j(\ell) = \tilde{\phi}_m(\ell)$. In particular, we have $m \in S_j$.

Let $w_m = \ell p^m + h$ and let κ_m be the partition of w_m consisting of $k - A_m$ copies of n and 1 copy of b_m . By Proposition 3.2 we see that λ has at most one element not equal to n . Since λ is a partition of w_m , and

$$w_m = \phi_j(\ell) - i_m + h = (k - A_m)n + b_m,$$

it follows that $\lambda = \kappa_m$. Hence $c_\lambda = c_{\kappa_m} = c_n^{k-A_m} c_{b_m}$ and $\bar{v}_p(b_m) = \bar{v}_p(\lambda_q) = t$. Using equation (4.1) and Proposition 4.2 we get

$$\hat{c}_h \equiv c_h + \sum_{m \in S_j} d_{\kappa_m \mu_{p^m}} c_n^{k-A_m} c_{b_m} r^{p^m} \pmod{\mathcal{M}_K^{k+1}}. \quad (4.2)$$

Let $m \in S_j$. Since

$$j = \bar{v}_p(\phi_j(\ell)) = \bar{v}_p(\tilde{\phi}_m(\ell)) = \bar{v}_p(i_m + \ell p^m)$$

and $m \leq j$ we get $m \leq \bar{v}_p(i_m) = \bar{v}_p(b_m)$. Hence $b'_m = b_m/p^m$ is an integer. Let κ'_m be the partition of

$$w'_m = (k - A_m)up^{\nu-m} + b'_m = h_0 p^{j-m} + \ell$$

consisting of $k - A_m$ copies of $up^{\nu-m}$ and 1 copy of b'_m . Let μ'_{p^m} be the partition of w'_m consisting of $h_0 p^{j-m} - 1$ copies of 1 and 1 copy of $\ell + 1$. Since $h \leq n$ we have $up^{\nu-m} > h_0 p^{j-m} - 1$. Hence if $b'_m \neq up^{\nu-m}$ then we can compute $d_{\kappa'_m \mu'_{p^m}}$ using Proposition 2.3.

Suppose $b_m < h$. Then $h_0 p^{j-m} - 1 \geq b'_m$, so by Proposition 2.3 we get

$$d_{\kappa'_m \mu'_{p^m}} = (-1)^{k+\ell+A_m} (h_0 p^{j-m} + \ell - up^{\nu-m}).$$

Suppose $h \leq b_m < n$. Then $h_0 p^{j-m} - 1 < b'_m$, so by Proposition 2.3 we get

$$d_{\kappa'_m \mu'_{p^m}} = (-1)^{k+\ell+A_m} (h_0 p^{j-m} + \ell).$$

Suppose $b_m = n$, so that $b'_m = up^{\nu-m}$. Since $up^{\nu-m} > h_0 p^{j-m} - 1$, the only cycle digraph which admits a (κ'_m, μ'_{p^m}) -tiling consists of a single cycle Γ of length w'_m . By Proposition 2.2(a) we get $\eta_{\kappa'_m \mu'_{p^m}}(\Gamma) = up^{\nu-m}$. It then follows from (2.1) that

$$d_{\kappa'_m \mu'_{p^m}} = (-1)^{k+\ell+A_m} up^{\nu-m}.$$

Hence in all three cases we have $d_{\kappa'_m \mu'_{p^m}} = g_m$.

Since $m \leq t \leq \nu$ it follows from (3.2) and (3.1) that

$$\begin{aligned} i_m &\leq i_t^{\pi_L} + (t - m)e_L \\ nA_m - b_m &\leq nv_K(c_{b_m}) - b_m + (t - m)e_L \\ A_m &\leq v_K(c_{b_m}) + (t - m)e_K \\ k + 1 &\leq k - A_m + v_K(c_{b_m}) + (t - m + 1)e_K. \end{aligned} \quad (4.3)$$

Since $p^t \mid b_m$ we have $p^{t-m} \mid b'_m$. Therefore by Proposition 2.5 we get

$$d_{\kappa_m \mu_{p^m}} \equiv d_{\kappa'_m \mu'_{p^m}} \pmod{p^{t-m+1}}.$$

Using (4.3) we see that

$$\begin{aligned} d_{\kappa_m \mu_{p^m}} c_n^{k-A_m} c_{b_m} &\equiv d_{\kappa'_m \mu'_{p^m}} c_n^{k-A_m} c_{b_m} \pmod{\mathcal{M}_K^{k+1}} \\ &\equiv g_m c_n^{k-A_m} c_{b_m} \pmod{\mathcal{M}_K^{k+1}}. \end{aligned}$$

Therefore the theorem holds when $\tilde{\pi}_L = \hat{\pi}_L$.

We now prove the theorem in the general case. We may assume that

$$\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{M}_L^{\ell+2}}.$$

It follows that $\tilde{\pi}_L \equiv \hat{\pi}_L \pmod{\mathcal{M}_L^{\ell+2}}$, so by Theorem 4.3 we get $\tilde{c}_h \equiv \hat{c}_h \pmod{\mathcal{M}_K^{\rho_h(\ell+1)}}$. Since $(\phi_j(\ell) + h)/n = k$ and $\phi_j(\ell + 1) > \phi_j(\ell)$ this implies $\tilde{c}_h \equiv \hat{c}_h \pmod{\mathcal{M}_K^{k+1}}$. Hence the theorem holds for $\tilde{\pi}_L$. \square

Remark 4.6 Suppose $\bar{v}_p(\phi_j(\ell)) = j' \leq j$. Then $\phi_j(\ell) = \phi_{j'}(\ell)$. In particular, $\phi_\nu(\ell) = \phi_{j'}(\ell)$ with $j' = \bar{v}_p(\phi_\nu(\ell))$. Hence if $1 \leq h \leq n$ and n divides $\phi_\nu(\ell) + h$ then Theorem 4.5 gives a congruence for \tilde{c}_h modulo \mathcal{M}_K^{k+1} , where $k = (\phi_\nu(\ell) + h)/n$. This is the congruence obtained by Krasner [7, p.157]. If ℓ is greater than or equal to the largest lower ramification break of L/K then $\phi_j(\ell) = \phi_\nu(\ell)$ for $0 \leq j \leq \nu$. Therefore Theorem 4.5 does not extend [7] in these cases.

5 Some examples

In this section we give two examples related to the theorems proved in Section 4. We first apply these theorems to a 3-adic extension of degree 9:

Example 5.1 Let K be a finite extension of the 3-adic field \mathbb{Q}_3 such that $v_K(3) \geq 2$. Let

$$f(X) = X^9 - c_1 X^8 + \cdots + c_8 X - c_9$$

be an Eisenstein polynomial over K such that $v_K(c_2) = v_K(c_6) = 2$, $v_K(c_h) \geq 2$ for $h \in \{1, 3\}$, and $v_K(c_h) \geq 3$ for $h \in \{4, 5, 7, 8\}$. Let π_L be a root of $f(X)$. Then $L = K(\pi_L)$ is a totally ramified extension of K of degree 9, so we have $u = 1$, $\nu = 2$. It follows from our assumptions about the valuations of the coefficients of $f(X)$ that the indices of inseparability of L/K are $i_0 = 16$, $i_1 = 12$, and $i_2 = 0$. Therefore $A_0 = 2$, $A_1 = 2$, $A_2 = 1$, and $b_0 = 2$, $b_1 = 6$, $b_2 = 9$. We get the following values for $\tilde{\phi}_j(\ell)$ and $\phi_j(\ell)$:

ℓ	$\tilde{\phi}_0(\ell)$	$\tilde{\phi}_1(\ell)$	$\tilde{\phi}_2(\ell)$	$\phi_0(\ell)$	$\phi_1(\ell)$	$\phi_2(\ell)$
1	17	15	9	17	15	9
2	18	18	18	18	18	18
3	19	21	27	19	19	19

Now let $\tilde{\pi}_L$ be another uniformizer for L , with minimum polynomial

$$\tilde{f}(X) = X^9 - \tilde{c}_1 X^8 + \cdots + \tilde{c}_8 X - \tilde{c}_9.$$

Suppose $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{M}_L^2}$. Then by Theorem 4.3 we get $\tilde{f} \sim_1 f$. Using the table above we find that

$$\begin{aligned} \tilde{c}_h &\equiv c_h \pmod{\mathcal{M}_K^2} \text{ for } h \in \{1, 3, 9\}, \\ \tilde{c}_h &\equiv c_h \pmod{\mathcal{M}_K^3} \text{ for } h \in \{2, 4, 5, 6, 7, 8\}. \end{aligned}$$

This is an improvement on [7], which gives $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^2}$ for $1 \leq h \leq 9$. If $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{M}_L^3}$ we get $\tilde{f} \sim_2 f$, and hence $\tilde{c}_h \equiv c_h \pmod{\mathcal{M}_K^3}$ for $1 \leq h \leq 9$. If $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{M}_L^4}$ we get $\tilde{f} \sim_3 f$, and hence

$$\begin{aligned} \tilde{c}_h &\equiv c_h \pmod{\mathcal{M}_K^3} \text{ for } 1 \leq h \leq 8, \\ \tilde{c}_9 &\equiv c_9 \pmod{\mathcal{M}_K^4}. \end{aligned}$$

Since the largest lower ramification break of L/K is 2, the congruences we get for $\ell \geq 2$ are the same as those in [7].

Suppose $\tilde{\pi}_L \equiv \pi_L + r\pi_L^2 \pmod{\mathcal{M}_L^3}$, with $r \in \mathcal{O}_K$. By the table above we get $\bar{v}_3(\phi_0(1)) = 0$, $\bar{v}_3(\phi_1(1)) = 1$, $\bar{v}_3(\phi_2(1)) = 2$ and $S_0 = \{0\}$, $S_1 = \{1\}$, $S_2 = \{2\}$. The corresponding values of h are 1, 3, 9, and we have $h_0 = 1$, $k = 2$ in all three cases. By applying Theorem 4.5 with $\ell = 1$, $j = 0, 1, 2$ we get the following congruences:

$$\begin{aligned} \tilde{c}_1 &\equiv c_1 + (-1)^{2+1+2}(1+1)c_2r \pmod{\mathcal{M}_K^3} \\ &\equiv c_1 - 2c_2r \pmod{\mathcal{M}_K^3} \\ \tilde{c}_3 &\equiv c_3 + (-1)^{2+1+2}(1+1)c_6r^3 \pmod{\mathcal{M}_K^3} \\ &\equiv c_3 - 2c_6r^3 \pmod{\mathcal{M}_K^3} \\ \tilde{c}_9 &\equiv c_9 + (-1)^{2+1+1}c_9^2r^9 \pmod{\mathcal{M}_K^3} \\ &\equiv c_9 + c_9^2r^9 \pmod{\mathcal{M}_K^3}. \end{aligned}$$

Only the congruence for \tilde{c}_9 follows from [7].

Suppose $\tilde{\pi}_L \equiv \pi_L + r\pi_L^3 \pmod{\mathcal{M}_L^4}$. Then $\bar{v}_3(\phi_2(2)) = 2$ and $S_2 = \{0, 1, 2\}$, which gives $h = 9$, $h_0 = 1$, and $k = 3$. By applying Theorem 4.5 with $\ell = 2$, $j = 2$ we get the following congruence:

$$\begin{aligned} \tilde{c}_9 &\equiv c_9 + (-1)^{3+2+2}(9+2-9)c_9c_2r \\ &\quad + (-1)^{3+2+2}(3+2-3)c_9c_6r^3 + (-1)^{3+2+1}c_9^2c_9r^9 \pmod{\mathcal{M}_K^4} \\ &\equiv c_9 - 2c_2c_9r - 2c_6c_9r^3 + c_9^3r^9 \pmod{\mathcal{M}_K^4}. \end{aligned}$$

Suppose $\tilde{\pi}_L \equiv \pi_L + r\pi_L^4 \pmod{\mathcal{M}_L^5}$. Then $\bar{v}_3(\phi_0(3)) = 0$ and $S_0 = \{0\}$, so we get $h = 8$, $h_0 = 8$, and $k = 3$. By applying Theorem 4.5 with $\ell = 3$, $j = 0$ we get the following congruence:

$$\begin{aligned} \tilde{c}_8 &\equiv c_8 + (-1)^{3+3+2}(8+3-9)c_9c_2r \pmod{\mathcal{M}_K^4} \\ &\equiv c_8 + 2c_2c_9r \pmod{\mathcal{M}_K^4}. \end{aligned}$$

Again, since the largest lower ramification break of L/K is 2, the congruences we get for $\ell \geq 2$ are the same as those in [7]. \square

One might hope to prove the following converse to Theorem 4.3: If $\pi_L, \tilde{\pi}_L$ are uniformizers for L whose minimum polynomials satisfy $\tilde{f} \sim_\ell f$, then there is $\sigma \in \text{Aut}_K(L)$ such that $\sigma(\tilde{\pi}_L) \equiv \pi_L \pmod{\mathcal{M}_L^{\ell+1}}$. The example below shows that this is not necessarily the case:

Example 5.2 Let π_L be a root of the Eisenstein polynomial $f(X) = X^4 + 6X^2 + 4X + 2$ over the 2-adic field \mathbb{Q}_2 . Then $L = \mathbb{Q}_2(\pi_L)$ is a totally ramified extension of \mathbb{Q}_2 of degree 4, with indices of inseparability $i_0 = 5$, $i_1 = 2$, and $i_2 = 0$. We get the following values for $\tilde{\phi}_j(\ell)$ and $\phi_j(\ell)$:

ℓ	$\tilde{\phi}_0(\ell)$	$\tilde{\phi}_1(\ell)$	$\tilde{\phi}_2(\ell)$	$\phi_0(\ell)$	$\phi_1(\ell)$	$\phi_2(\ell)$
1	6	4	4	6	4	4
2	7	6	8	7	6	6
3	8	8	12	8	8	8

Set $\tilde{\pi}_L = \pi_L + \pi_L^2$, and let the minimum polynomial for $\tilde{\pi}_L$ over \mathbb{Q}_2 be

$$\tilde{f}(X) = X^4 - \tilde{c}_1 X^3 + \tilde{c}_2 X^2 - \tilde{c}_3 X + \tilde{c}_4.$$

By Theorem 4.3 we have $\tilde{f} \sim_1 f$, and hence

$$\begin{aligned} \tilde{c}_1 &\equiv 0 \pmod{4} \\ \tilde{c}_2 &\equiv 6 \pmod{4} \\ \tilde{c}_3 &\equiv -4 \pmod{8} \\ \tilde{c}_4 &\equiv 2 \pmod{4}. \end{aligned}$$

Theorem 4.5 gives a refinement of the last congruence:

$$\begin{aligned} \tilde{c}_4 &\equiv 2 + (-1)^{2+1+1}(2+1-2) \cdot 2^{2-1} \cdot 6 + (-1)^{2+1+1} \cdot 2^{2-1} \cdot 2 \pmod{8} \\ &\equiv 2 \pmod{8}. \end{aligned}$$

Using this refinement we get $\tilde{f} \sim_2 f$.

Using [5] (see also Table 4.2 in [4]) we obtain a list of the degree-4 extensions of \mathbb{Q}_2 . Using the data in this list we find that L/\mathbb{Q}_2 is not Galois, and the only quadratic subextension of L/\mathbb{Q}_2 is M/\mathbb{Q}_2 , where $M = \mathbb{Q}_2(\sqrt{-1})$. Hence $\text{Aut}_{\mathbb{Q}_2}(L) = \text{Gal}(L/M)$. Since the lower ramification breaks of L/\mathbb{Q}_2 are 1, 3, and the lower ramification break of M/\mathbb{Q}_2 is 1, the lower ramification break of L/M is 3. Hence if $\sigma \in \text{Aut}_{\mathbb{Q}_2}(L)$ then $\sigma(\tilde{\pi}_L) \equiv \tilde{\pi}_L \pmod{\mathcal{M}_L^4}$. Since $\tilde{\pi}_L = \pi_L + \pi_L^2$ we get $\sigma(\tilde{\pi}_L) \not\equiv \pi_L \pmod{\mathcal{M}_L^3}$. \square

References

- [1] M. Fried, Arithmetical properties of function fields II, The generalized Schur problem, *Acta Arith.* **25** (1973/74), 225–258.
- [2] M. Fried and A. Mézard, Configuration spaces for wildly ramified covers, appearing in *Arithmetic Fundamental Groups and Noncommutative Algebra*, Proc. Sympos. Pure Math. **70** (2002), 353–376.
- [3] V. Heiermann, De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux, *J. Number Theory* **59** (1996), 159–202.
- [4] J. Jones and D. Roberts, A database of local fields, *J. Symbolic Comput.* **41** (2006), 80–97.
- [5] J. Jones and D. Roberts, Database of Local Fields, retrieved 31 December 2016 from <https://math.la.asu.edu/~jj/localfields/>.
- [6] K. Keating, Extensions of local fields and elementary symmetric polynomials, [arXiv:1608.07350](https://arxiv.org/abs/1608.07350) [math.NT].
- [7] M. Krasner, Sur la primitivité des corps \mathfrak{P} -adic, *Mathematica (Cluj)* **13** (1937), 72–191.
- [8] A. Kulikaukas and J. Remmel, Lyndon words and transition matrices between elementary, homogeneous and monomial symmetric functions, *Electronic J. Combinatorics* **13** (2006), #R18.
- [9] J.-P. Serre, *Corps Locaux*, Hermann, Paris (1962).